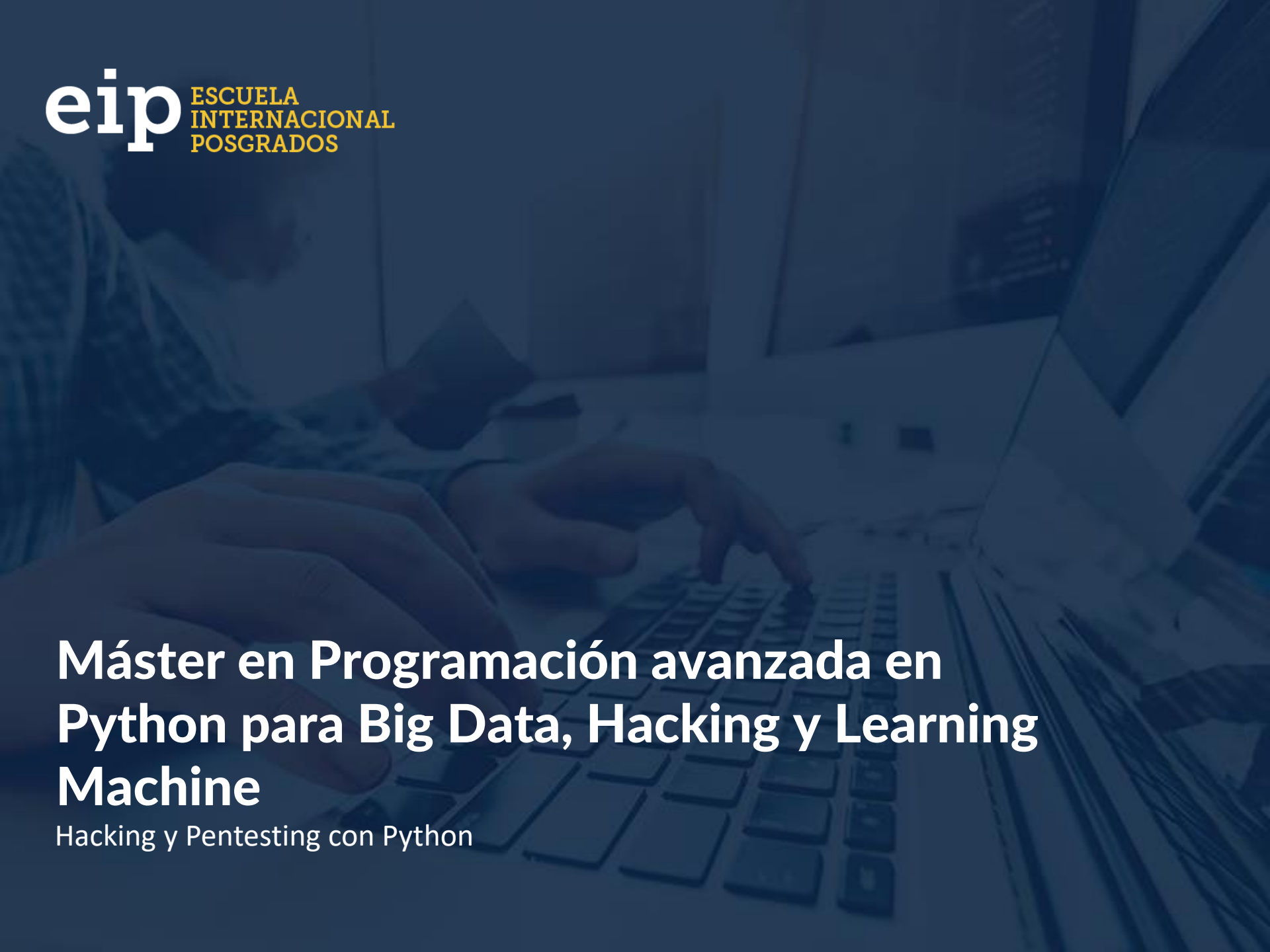

eip ESCUELA INTERNACIONAL POSGRADOS

Máster en Programación avanzada en Python para Big Data, Hacking y Learning Machine

Hacking y Pentesting con Python

MÓDULO 07

Rutinas de Red Teaming con Python.

Características de la red anónima TOR.

Red que provee unos niveles de anonimato fuertes gracias al uso de una red distribuida en Internet que utiliza el protocolo TOR.

Se puede usar el modo “outproxy” para salir a Internet utilizando los repetidores que se encuentran en la red de TOR.

Se puede utilizar en modo “inproxy” para navegar por la web profunda de Tor.

Amplio soporte por parte de la comunidad de contribuidores y desarrolladores del proyecto. Estable, robusto y con una trayectoria de más de casi 20 años.

Instancias de TOR.

El software de TOR se distribuye en dos versiones: La instancia que se puede configurar e instalar manualmente y TorBrowser.

Cualquiera de las dos alternativas es valida, sin embargo, en ocasiones suele ser mejor utilizar una instancia de TOR que se instala como servicio en el sistema.

En ambos casos es necesario editar el fichero de configuración "torrc" para indicar las opciones de configuración más adecuadas.

TorBrowser cuenta con una configuración por defecto que suele ser aceptable en la mayoría de los casos.

Instancias de TOR.

Si un cliente desea acceder a un servicio oculto en la deep web de TOR, tiene que estar correctamente configurado para conectarse a la red.

Todos los clientes tienen que usar el proxy SOCKS de una instancia de TOR para poder conectarse a la red de TOR.

Se puede configurar cualquier navegador web para utilizar TOR, sin embargo se recomienda utilizar TorBrowser, ya que viene con una instancia de TOR preconfigurada y preparada para conectarse con la red.

Anonimato con TOR y Python

Existen varias librerías en Python para acceso y control de instancias de TOR. A continuación se listan algunas de ellas.

SocksiPy: Es la principal librería en Python para realizar conexiones por medio de un proxy SOCKS.

Requests: Permite ejecutar peticiones HTTP por medio de un proxy SOCKS.

Stem y Txtorcon: Son las principales alternativas para controlar instancias de TOR

Stem: Librería sincrona, aprovecha protocolo de control.

Txtorcon: Librería asíncrona, aprovecha protocolo de control.

Librería STEM

Librería de acceso programático utilizando el protocolo de control de TOR. Permite ejecutar todas las operaciones definidas en el protocolo y de ésta forma, administrar de forma automática el comportamiento de una instancia de TOR.

Permite hacer consultas y cambios en caliente a una instancia de TOR.

Funciones y métodos para consultar detalles de configuración a las autoridades de directorio de TOR.

Permite levantar y detener una instancia de TOR desde cualquier script en Python.

MUCHAS GRACIAS POR SU ATENCIÓN

eip ESCUELA INTERNACIONAL POSGRADOS

decheverri@grupomainjobs.com

LINKEDIN

Daniel Echeverri
https://www.linkedin.com/in/adastra1/

twitter.com/eiposgrados

facebook.com/eiposgrados

instagram.com/eiposgrados